Remarks

Changes

The specification has been amended on page 7 to correct the misspelling noted by the Examiner. The specification has also been amended on page 9 to correct another error noted by applicants.

Claim 1 has essentially been split into two claims: the first (claim 1 as amended) directed to device authentication and the second (new claim 23, discussed below, as well as dependent claim 13) directed to electronic signature generation and verification. More particularly, claim 1 as amended is directed to a method in which a first "device authentication" (page 4, line 23) is performed between the input device and the "memory device" (original claim 6) when writing digital data from the input device to the memory device, while a second "device authentication" (page 6, line 18) is performed between the memory device and the receiving device when transferring the digital data from the memory device to the receiving device.

Claims 2 and 8, dependent on claim 1, have been amended to agree with the changes in claim 1.

Claim 3 has been amended to recite that the second device authentication is performed by a central processing unit (CPU 220) built into the memory device.

Claim 4 has been amended to recite that the digital data is transferred as authenticated data if the first and second device authentications are successful and is transferred as ordinary data if the first and second device authentications are not successful (page 3, lines 14-15; page 5, lines 4-7 and 15-17; page 11, lines 13-15).

Claim 5 has been amended to recite that the first device authentication is performed using a first encryption function (Hdc) and key (Kdc) and that the second device authentication is performed using a second encryption function (Hpc) and key (Kpc).

Claims 6, 7 and 9 have been cancelled.

New claim 10, dependent on claim 1, recites that each of the device authentications involves having a first device ascertain that a second device possesses a secret value (Kdc, Kpc) corresponding to a value held by the first device.

New claim 11, dependent on claim 10, recites further that the first device is a recipient of digital data from the second device.

New claim 12, dependent on claim 1, recites that each of the device authentications involves the exchange of an authentication value generated independently of the digital data.

New claim 13 recites the further steps, claimed independently in claim 23, of generating an electronic signature on digital data when writing the digital data from the input device to the memory device and authenticating the electronic signature on the digital data when transferring said digital data from the memory device to the receiving device.

New claim 14 is directed to a program storage device for performing the method steps of claim 1.

New claims 15, 16 and 17 are similar to claims 1, 3 and 5 as amended, but are in apparatus form. New claims 18 and 19 are similar to cancelled claims 6 and 7, but depend on apparatus claim 15. New claim 20 is similar to claim 13, but depends on apparatus claim 15.

Claim 21 is similar to claims 1 and 15, but is directed to a memory device. New claim 22 is similar to claims 13 and 20, but depends on device claim 21.

Claim 23 is based upon the part of original claim 1 relating to image authentication and claimed dependently in new claim 13. More particularly, new claim 23 is directed to a method for authenticating digital data in a system for writing digital data entered from an input device to a memory device and transferring the digital data written in the memory device to a receiving device in which the memory device generates an electronic signature on digital data when writing the digital data from the input device to the memory device and authenticates[1] the electronic signature on the digital data when transferring the digital data from the memory device to the receiving device.

Dependent claim 24, modeled after claim 5 as amended, recites that the memory device has a hash function (Hcf) and an internal key (Kcf) for generating the electronic signature.

Dependent claim 25 is directed to a program storage device.

Claim 26 is similar to new claim 23, but is directed to apparatus.

Claims 27 and 28 are modeled after claims 3 and 5 as amended, but are dependent on claim 26.

Finally, claims 29 and 30 are modeled after cancelled claims 6 and 9, but are dependent on claim 26.

Rejections under 35 U.S.C. § 112

Claims 1-3 and 5 stand rejected under § 112, second paragraph, on the ground that they allegedly "fail to include definitive steps that must be performed" and "seem to be reciting capabilities rather than actions performed" (page 2, ¶ 3(a)).

As amended, claim 1 is believed to avoid any ground for rejection under 35 U.S.C. § 112, second paragraph. Claim 1 recites that a first device authentication is performed when writing digital data from the input device to the memory device and that a second device authentication is performed when transferring the digital data from the memory device to the receiving device. These steps of performing device authentication are not just "capabilities" of the system, but are positive acts that are definitely performed in the claimed method. As for the conjunction "when", it is being used in its obvious sense of linking the occurrence of one event (performing a device

[1] The original abstract says that the electronic signature "is decrypted so as to transfer the digital data after ensuring that it has not been changed since it was recorded" (page 15, lines 10-11).

authentication) to another (writing or transferring digital data). Its use here is thus clearly proper and does not detract from the definiteness of the actions being performed.

Claims 2, 3 and 5 as amended similarly comply with § 112, second paragraph. Claim 2 recites the positive step of mixing authentication data into the digital data transferred between devices. Claim 3 recites how the second device authentication is performed, while claim 5 recites how digital data is transferred. In each case, positive acts are recited, not mere capabilities.

Claim 3 also stands rejected under § 112, second paragraph, on account of its recital of an implementing step is allegedly already recited in claim 1 (page 2, ¶ 3(b)). As amended, claim 3 describes only how the second device authentication of claim 1 is performed and does not purport to introduce an additional step. Accordingly, claim 3 as amended should avoid this ground for rejection under § 112.

Claims 6, 7 and 9, rejected under § 112, second paragraph, for containing "apparatus limitations" (page 2, ¶ 3(c)), have been cancelled as method claims. (Similar claims have been added as apparatus claims.)

Claim 4, dependent on claim 1, has been rejected under 35 U.S.C. § 112, fourth paragraph, for "failing to set forth and specify a further limitation of the subject matter claimed", specifically for appearing "to remove steps of claim 1 rather than adding an additional limitation" (page 2, ¶ 4). Claim 4 as amended recites that the digital data is processed as authenticated data if the first and second device authentications are successful and is processed as ordinary data if the first and second device authentications are not successful. The amended claim is therefore saying only that the digital data is processed differently, depending on the results of device authentication, not that it is not being processed. Accordingly, there is no conflict between claim 4 as amended and § 112.

Rejections under 35 U.S.C. 103

As amended, the claims are also believed to distinguish patentably over the references cited by the Examiner. Remarks on specific sets of claims follow.

1. Claims 1-5, 8 and 10-22

Each of these claims is directed to an implementation in which a first device authentication is performed between an input device and an memory device when writing digital data from the input device to the memory device, while a second device authentication is performed between the memory device and the receiving device when transferring the digital data from the memory device to the receiving device. These claims are thus directed to device authentication, which seeks to determine whether an interacting device is what it purports to be. This differs fundamentally from the data or image authentication disclosed in the references.

The first of these references, Friedman U.S. Patent 5,499,294, discloses a digital camera system in which the camera itself uses a private signature key to generate a digital signature that is stored along with the image in memory. An entity seeking to authenticate the image uses the corresponding public key to verify the signature using standard public-key signature verification techniques.

The other cited reference, Steinberg U.S. Patent 6,510,520, discloses a digital camera system in which a secure storage device 10 (Fig. 1) intermediating between a camera and a user's computer is used to either encrypt a digital image or generate a signature on the image. The ultimate user, not the secure storage device, either decrypts the image or authenticates the digital signature, depending on the type of processing performed by the secure storage device.

In each of these systems, what is authenticated is the digital image itself, and not the device that is the source or the destination of the image. As compared with device authentication (which may involve, for example, encrypting a random number), however, image authentication is generally a more computationally intensive task, since the authentication value is preferably generated on the entire image. Also, problems may result if image authentication alone is used as a validation mechanism and the original image is a counterfeit image. Thus, in the Steinberg system, if the original camera is arranged to provide a counterfeit image, the secure storage device 10 would have no way of knowing this and would proceed to sign or encrypt the image in the usual manner, oblivious to the fact that the original image is counterfeit. Similarly, in the Friedman system, the public key used to verify the digital signature is helpfully supplied by the digital camera itself. Since anyone can generate a public-private key pair, a rogue operator could falsify an image (or have one pre-stored) within the camera itself. However, as long as the decryption or signature procedure is successful, a downstream entity would have no way of knowing that the image was counterfeit.

In sum, the cited references teach only image authentication and not device authentication as claimed by applicants. As a consequence, they rely on authentication of the image itself and fail to detect security failures resulting from an untrustworthy entity providing a falsified image. Accordingly, claims 1-5, 8 and 10-22, which are directed to device authentication, clearly distinguish patentably over the references cited.

Claim 10 is additionally believed to distinguish patentably over the art cited by virtue of its recitation that each of the device authentications involves having a first device ascertain that a second device possesses a secret value corresponding to a value held by the first device. Claim 11, dependent on claim 10, is additionally believed to distinguish patentably over the art cited for this reason and by virtue of its recitation that the first device is a recipient of digital data from the second device.

Claim 11 is additionally believed to distinguish patentably over the art cited by virtue of its recitation that each of the device authentications involves the exchange of an authentication value generated independently of the digital data.

Claims 13, 20 and 22 are additionally believed to distinguish patentably over the art cited by virtue of their recitations relating to electronic signature generation and authentication by the memory device, as discussed below in conjunction with claims 23-30.

Claims 23-30

Claims 23-30 are directed to implementations in which a memory device generates an electronic signature on digital data when writing digital data from an input device and authenticates the electronic signature on the digital data when transferring the digital data to a receiving device. These claims thus distinguish over the systems described in the references cited, in which the entity authenticating an electronic signature is downstream of the entity generating the signature. By having the memory device itself authenticate the signature when transferring the data from the memory device downstream, especially by using its own internal key as recited in claims 24, 28, and 29, applicants are able to prevent the storage area of the memory device from being compromised and replaced by changed data (page 11, lines 7-9). Accordingly, this group of claims is likewise believed to distinguish patentably over the art cited.

Conclusion

For the foregoing reasons, claims 1-5 and 8 as amended and new claims 10-30 are believed to distinguish patentably over the art cited by the Examiner. Reconsideration of the application as amended is respectfully requested. It is hoped that upon such consideration, the Examiner will hold all claims allowable and pass the case to issue at an early date. Such action is earnestly solicited.

Respectfully submitted,
KOICHI KAMIJO et al.

By

William A. Kinnaman, Jr.
Registration No. 27,650
Phone: (845) 433-1175
Fax: (845) 432-9601

WAK/wak